I CLAIM:

1. A system for a secure key distribution protocol in AAA for Mobile IP, comprising:

a MN that is configured to: generate a Reg-Req message that includes Diffie-Hellman parameters that are used to generate session keys and produce signatures; initiate an authentication session by sending the Reg-Req message; receive a Reg-Reply message that includes session keys that may be used to directly communicate with the AAAH, AAAF, HA, and FA nodes while the MN is in a foreign authority;

a FA that is configured to: receive the Reg-Req message; ensure that the authentication session is valid; and when valid, sign and send the Reg-Req message; otherwise, end the authentication session; receive, authenticate, decrypt, sign, and send the Reg-Reply message to the MN;

an AAAF that is configured to: receive and authenticate the Reg-Req message; generate the session keys using the Diffie-Helman algorithm and the Diffie-Hellman parameters; add an identifier relating to the Reg-Req message; sign and send the Reg-Req message; receive, authenticate, sign and send the Reg-Reply message to the FA;

an AAAH that is configured to: receive and authenticate the Reg-Req message; sign and send the Reg-Req message; receive and authenticate the Reg-Reply message; encrypt the session keys; sign and send the Reg-Reply message to the AAAF;

a HA that is configured to: receive the Reg-Req message; prepare a Reg-Reply message in response to the Reg-Req message; and send the Reg-Reply message to the AAAH.

2. The system of Claim 1, wherein the Diffie-Hellman parameters include an n, a g, and a p parameter; wherein the parameters are used to generate the session keys and are used in signing the Reg-Req message and the Reg-Reply message.

3. The system of Claim 2, wherein the Reg-Req message and the Reg-Reply message includes an identifier relating to where the message originated, wherein the identifier is selected from an NAI and a new random nonce.

4. The system of Claim 3, wherein the Reg-Req message and the Reg-Reply message are signed using a security association between a sender of the Reg-Req message and the Reg-Reply message and a receiver of the Reg-Req message and the Reg-Reply message.

5. The system of Claim 4, wherein the AAAF is further configured to: choose a secret random number y to calculate a parameter $q = g^y \bmod n$ according to the Diffie-Helman algorithm that is used in generating the session keys.

6. The system of Claim 4, wherein authenticating the Reg-Req message and the Reg-Reply message further comprises ensuring that the Reg-Req message and the Reg-Reply message came from the sender by checking the signature relating to a security association between the sender and the receiver.

7. The system of Claim 6, wherein the AAAF is further configured to determine the AAAH for the MN in response to the identifier associated with the MN.

8. The system of Claim 7, wherein the AAAF is further configured to store a time associated with the initiation of the authentication session in order to prevent a Reply message fail.

9. The system of Claim 8, wherein the AAAH is further configured to protect the authentication process from a replay attack, and when the AAAH does not recognize the MN, generate an error.

10. The system of Claim 9, wherein the AAAH is further configured to help the FA directly communicate to the HA through a security association by generating the

session keys for the FA, HA, and MN, and distributing the session keys in a secure fashion.

11. The system of Claim 10, wherein distributing the session keys in a secure fashion, further comprises encrypting the session keys.

12. The system of Claim 11, wherein the HA is further configured to register a current location of the MN and store the session keys.

13. A method for a secure key distribution protocol in AAA for Mobile IP, comprising:

establishing secure associations between a MN, an AAAH, an AAAF, a HA, and a FA to help ensure secure communication;

securing a Reg-Req message and a Reg-Reply message used in establishing the secure associations;

creating session keys; and

distributing the session keys in a secure manner.

14. The method of Claim 13, further comprising using a home authority and a foreign authority to maintain and help establish the secure associations;

15. The method of Claim 14, wherein establishing the secure associations between the MN, the AAAH, the AAAF, the HA, and the FA, further comprises:

establishing a secure association between the MN and the AAAH;
establishing a secure association between the AAAH and the HA;
establishing a secure association between the AAAF and the AAAH;
establishing a secure association between the AAAF and the FA; and
establishing a secure association between the AAAF and the MN.

16. The method of Claim 15, further comprising determining when a signature is an authentic signature based on the secure associations and the session keys.

17. The method of Claim 16, wherein establishing the secure associations between the MN, the AAAH, the AAAF, the HA, and the FA to help ensure secure communication, further comprises:

signing the Reg-Req message and the Reg-Reply message using the session keys; and

authenticating the received Reg-Req message and the Reg-Reply message.

18. The method of Claim 17, wherein creating the session keys further comprises utilizing Diffie-Hellman parameters and the Diffie-Hellman algorithm.

19. The method of Claim 18, wherein the Reg-Req message includes an NAI associated with the MN, a timestamp, a challenge issued by the FA, and the Diffie-Hellman parameters.

20. The method of Claim 19, wherein the Reg-Reply message includes an identifier and the session keys.